

# Outline for April 7, 2005

Reading: §13, 4.1–4.5

## Discussion

Two MIT graduate students bought a number of used hard drives on E-Bay and analyzed them. They were able to recover lots of files, including files containing very personal information (such as a love letter), and in some cases even restore the operating system of the computer to which the hard drive belonged. Some of these disks had simply been discarded, but others had files deleted, or were reformatted—and still the students could recover the files!

The news article said that the students' results showed how unaware people were of security issues. Is the data being on the discarded disks in fact a vulnerability? Are the “delete,” “rm,” “format,” and other such commands used to erase these disks secure? If not, what is the vulnerability in these programs, and how would you fix it?

## Outline

1. Principles of Secure Design
  - a. Principle of Least Privilege
  - b. Principle of Fail-Safe Defaults
  - c. Principle of Economy of Mechanism
  - d. Principle of Complete Mediation
  - e. Principle of Open Design
  - f. Principle of Separation of Privilege
  - g. Principle of Least Common Mechanism
  - h. Principle of Psychological Acceptability
2. Policy
  - a. Sets of authorized, unauthorized states
  - b. Secure systems in terms of states
  - c. Mechanism vs. policy
3. Types of Policies
  - a. Military/government vs. confidentiality
  - b. Commercial vs. integrity
4. Types of Access Control
  - a. Mandatory access control
  - b. Discretionary access control
  - c. Originator-controlled access control
5. High-Level Policy Languages
  - a. Characterization
  - b. Example: DTEL
6. Low-Level Policy Languages
  - a. Characterization
  - b. Example: Tripwire configuration file